МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

СОГЛАСОВАНО
Руководитель ОП
_____ Степанова А.А.
(подпись) (ФИО)

УТВЕРЖДАЮ
И.о. директора департамента
_____ Заболотский В.С.
(подпись) (ФИО)
«13» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Конечные поля

Направление подготовки 01.04.01 Математика
магистерская программа «Алгебра»
Форма подготовки очная

курс 1 семестр 1
лекции 34 час.
практические занятия 18 час.
самостоятельная работа студентов 92
в том числе с использованием МАО 18 час
контрольные работы не предусмотрены
всего часов аудиторной нагрузки 52 час.
в том числе с использованием МАО пр. 18 час.
зачет не предусмотрен
экзамен 1 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 10 января 2018 г. № 12 (с изменениями и дополнениями)

Рабочая программа обсуждена на заседании департамента математики, протокол № 1 от 13 сентября 2021 г.

И.о. директора департамента математики Заболотский В.С.
Составитель (ли): к.ф.-м.н, доцент С.Г.Чеканов

Владивосток

2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

Цель: знакомство студентов с современными концепциями и алгоритмами в теории конечных полей, их приложениями в теории информации и криптографии.

Задачи преподавания дисциплины:

- овладение основными концепциями современной теории конечных полей;
- ознакомление с современными алгоритмами в конечных полях;
- изучение основных понятий и конструкций для представления конечных полей;
- применение полученных знаний при изучении явлений природы и общества и исследование простейших процессов с помощью методов теории конечных полей.

Для успешного изучения дисциплины «Конечные поля» у обучающихся должны быть сформированы следующие предварительные компетенции

- способность видеть методологические аспекты построения математических теорий;
- применять системный подход в формализации математических задач;
- способностью к абстрактному мышлению, анализу, синтезу.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
научно-исследовательский	ПК-1 Способен к интенсивной научно-исследовательской работе	ПК-1.1 Ставит задачи, выбирает и применяет современные методы решения научных задач по тематике научных исследований, оценивает значимость получаемых результатов
		ПК-1.2 Критически анализирует и оценивает современные достижения и результаты деятельности по решению исследовательских и практических задач
		ПК-1.3 Принимает участие и выступает на научно-тематических конференциях
педагогический	ПК-3 Способен	ПК-3.1 Организует деятельность

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
	осуществлять обучение учебному предмету на основе использования предметных методик и современных образовательных технологий	учащихся, направленную на освоение программы, выбирает формы, методы и средства обучения математике, современные образовательные технологии, определяет методические закономерности их выбора
		ПК-3.2 Формулирует дидактические цели и задачи обучения математике и реализует их в образовательном процессе, разрабатывает программно-методическое обеспечение реализации программы обучения
		ПК-3.3 Применяет различные средства, методы и образовательные технологии обучения математике в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-1.1 Ставит задачи, выбирает и применяет современные методы решения научных задач по тематике научных исследований, оценивает значимость получаемых результатов	Знает новые научные результаты по выбранной тематике научных исследований
	Умеет правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы, оценивать значимость результатов с точки зрения их результативности и применимости
	Владеет навыками применения выбранных методов к решению научных задач
ПК-1.2 Критически анализирует и оценивает современные достижения и результаты деятельности по решению исследовательских и практических задач	Знает классические и современные методы решения задач по выбранной тематике научных исследований
	Умеет осуществлять отбор, систематизацию, анализ и оценку современных достижений для решения поставленных задач
	Владеет навыками критической оценки полученных результатов для обоснования выбора оптимальной стратегии решения исследовательских и практических задач
ПК-1.3 Принимает участие и выступает на научно-тематических конференциях	Знает способы представления научной информации при осуществлении академической и профессиональной коммуникации
	Умеет представлять и обсуждать новые достижения и научные результаты в рамках научно-тематических

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
	конференций
	Владеет навыками подготовки докладов и выступлений на научно-тематических конференциях
ПК-3.1 Организует деятельность учащихся, направленную на освоение программы, выбирает формы, методы и средства обучения математике, современные образовательные технологии, определяет методические закономерности их выбора	Знает концептуальные положения и требования к организации образовательного процесса по математике; особенности проектирования образовательного процесса по математике в образовательном учреждении высшего образования,
	Умеет проектировать элементы образовательной программы, рабочую программу преподавателя по математике; формулировать дидактические цели и задачи обучения математике и реализовывать их в образовательном процессе по математике;
	Владеет навыками планирования и проектирования образовательного процесса
ПК-3.2 Формулирует дидактические цели и задачи обучения математике и реализует их в образовательном процессе, разрабатывает программно-методическое обеспечение реализации программы обучения	Знает подходы к планированию образовательной деятельности; формы, методы и средства обучения математике
	Умеет обосновывать выбор методов обучения математике и образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых
	Владеет навыками определения дидактических целей и задач обучения математике, разработки учебно-методических материалов
ПК-3.3 Применяет различные средства, методы и образовательные технологии обучения математике в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых	Знает современные образовательные технологии, методические закономерности их выбора; особенности частных методик обучения математике
	Умеет планировать и комплексно применять различные средства обучения математике
	Владеет методами обучения математике и современными образовательными технологиями

Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 4 зачётные единицы (144 академических часа).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине являются:

Обозначение	Виды учебных занятий и работы обучающегося

Лек	Лекции
Пр	Практические работы
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА ЛЕКЦИИ (34 ЧАСА)

Тема 1. Введение (2 часа).

Группы, кольца, поля. Гомоморфизмы колец. Кольца многочленов.

Тема 2. Характеристика поля (4 часа).

Характеристика поля. Теорема о характеристике. Фактор кольцо по максимальному идеалу.

Тема 3. Простые расширения конечных полей (4 часа).

Кольцо многочленов от одной переменной над конечным полем. Неприводимые многочлены. Идеалы в кольце многочленов. Простые расширения и корни неприводимых многочленов.

Тема 4. Строение конечных полей (4 часа).

Подполя конечных полей. Теорема о существовании и единственности конечного поля.

Тема 5. Мультипликативная группа конечного поля (8 часа).

Теорема о примитивном элементе. Оценка числа примитивных элементов. Примитивные многочлены над конечным полем.

Тема 6. Линейные рекуррентные последовательности (8 часа)

Рекуррентные соотношения и регистры сдвига с обратной связью. Характеристический многочлен и матрица линейной рекуррентной последовательности. Оценка периода линейно рекуррентной последовательности, алгоритм Берлекемпа-Месси.

Тема 7. Алгебраические коды (4 часа).

Линейные пространства над конечными полями. Коды обнаруживающие и исправляющие ошибки.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Практические занятия (18 час.)

Занятие 1. Введение (1 час.)

1. Рассматриваются примеры группы, колец, полей.
2. Изучается алгоритм деления с остатком.
3. Теорема Безу. Основная теорема алгебры.
4. Гомоморфизмы колец и факторкольца. Алгоритм Евклида.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 2. Характеристика поля (2 час.)

1. Характеристика поля и ее влияние на арифметические и алгебраические свойства поля. Теорема о характеристике поля.
2. Конечное поле как линейное пространство. Различные представления элементов конечного поля.
3. Решение уравнений над конечными полями.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 3. Алгебраические расширения конечных полей (3 час.).

1. Построения простых расширений небольших конечных полей.
2. Кольцо многочленов от одной переменной над конечным полем.
3. Разложение многочленов на неприводимые множители.
4. Вычисление минимальных многочленов для элементов расширения.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 4. Строение конечных полей (3 час.).

1. Теорема о строении конечных полей.
2. Поле разложения многочлена.
3. Характеризация конечных полей с помощью кольца многочленов.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 5. Мультипликативная группа конечного поля (3 час.).

1. Теорема о примитивном элементе. Оценка числа примитивных элементов конечного поля.
2. Построение базисов алгебраических расширений конечных полей.
3. Представления элементов конечных полей.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 6. Линейные рекуррентные последовательности (3 час.).

1. Линейные рекуррентные последовательности над конечными полями.
2. Характеризация последовательностей с помощью рекуррентных соотношений.

3. Характеристический полином и сопровождающая матрица рекуррентной последовательности. Вычисление периода последовательности, алгоритм Берлекемпа-Месси.
4. Линейные группы и рекуррентные последовательности.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 7. Алгебраические коды и шифры над конечными полями (3 час.).

1. Построение кодов над конечными полями, оценка числа распознаваемых и исправляемых ошибок.
2. Создание генераторов ключевых последовательностей для поточных шифров.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Примеры самостоятельных работ

Тема: Алгоритм Евклида

Вариант 1.

Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов f и g с коэффициентами из указанного поля F:

$F = Q$,

$f(x) = x^7 + 2x^5 + 2x^2 - x + 2$,

$g(x) = x^6 - 2x^5 - x^4 + x^2 + 2x + 3$

Тема: Строение конечных полей

Вариант 1.

1. Показать, что для каждого конечного поля, кроме F_2, сумма всех его элементов равна 0.
2. Пусть a, b – элементы поля F_{2^n} (n – нечетное число). Показать, что из равенства $a^2 + ab + b^2 = 0$ вытекает $a = b = 0$.
3. Найти все примитивные элементы поля F_7.

Примеры индивидуальных домашних заданий

Тема: Алгоритм Евклида

Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов f и g с коэффициентами из указанного поля F:

(a) $F = Q$, $f(x) = x^7 + 2x^5 + 2x^2 - x + 2$, $g(x) = x^6 - 2x^5 - x^4 + x^2 + 2x + 3$;

(b) $F = F_2$, $f(x) = x^7 + 1$, $g(x) = x^5 + x^3 + x + 1$;

(c) $F = F_2, f(x) = x^5 + x + 1,\ g(x) = x^6 + x^5 + x^4 + 1;$
(d) $F = F_2, f(x) = x^5 + x^4 + 1,\ g(x) = x^4 + x^2 + 1;$
(e) $F = F_2, f(x) = x^5 + x^3 + x + 1,\ g(x) = x^4 + 1;$
(f) $F = F_2, f(x) = x^5 + x + 1,\ g(x) = x^4 + x^3 + 1;$
(g) $F = F_2, f(x) = x^5 + x^3 + 1,\ g(x) = x^4 + x + 1;$
(h) $F = F_3, f(x) = x^8 + 2x^5 + x^3 + x^2 + 1,$
(i) $g(x) = 2x^6 + x^5 + 2x^3 + 2x^2 + 2.$

Тема: Неприводимость многочленов над конечным полем

1. Построить таблицы сложения и умножения для факторкольца $F_2[x]/(x^3 + x^2 + x)$. Определить, будет ли это кольцо полем.
2. Пусть $[x + 1]$ – класс вычетов многочлена $x + 1$ в факторкольце $F_2[x]/\langle x^4 + 1\rangle$. Найти классы вычетов, составляющие главный идеал $\langle [x + 1]\rangle$ в указанном факторкольце.
3. Решить сравнение

$$(x^2 + 1)f(x) \equiv 1\big(mod(x^3 + 1)\big)$$

в $F_3[x]$, если это возможно.
4. Решить сравнение

$$(x^4 + x^3 + x^2 + 1)f(x) \equiv x^2 + 1\big(mod(x^3 + 1)\big)$$

в $F_2[x]$, если это возможно.

Тема: Алгебраические расширения конечного поля

1. Показать, что для многочлена f положительной степени над полем F следующие условия эквивалентны:
   (a) многочлен f неприводим над F;
   (b) главный идеал $\langle f\rangle$ кольца $F[x]$ является максимальным идеалом;
   (c) главный идеал $\langle f\rangle$ кольца $F[x]$ является простым идеалом.
2. Доказать, что если F_q - поле из q элементов, то $x^q - x = \prod_{a \in F_q}(x - a)$.

Тема: Представление элементов конечного поля с помощью многочленов

1. Найти число неприводимых унитарных многочленов степени 2 и 3 над полем Z_3.
2. Доказать, что при $a \in Z_p^*$ многочлен $x^p - x - a$ неприводим над Z_p.
3. Доказать, что при $a \neq 1$ многочлен $x^q - ax - b$ имеет в F_q корень.

4. Доказать, что $x^{2n} + x^n + 1$ неприводим над Z_2 тогда и только тогда, когда $n = 3^k$ для некоторого $k \geq 0$.
5. Доказать, что $x^{4n} + x^n + 1$ неприводим над Z_2 тогда и только тогда, когда $n = 3^k 5^m$ для некоторых целых $k, m \geq 0$.
6. Доказать, что многочлен $x^2 + 1$ неприводим над полем F_{11}, и показать непосредственно, что факторкольцо $F_{11}[x]/(x^2 + 1)$ состоит из 121 элемента. Доказать также, что многочлен $x^2 + x + 4$ неприводим над полем F_{11}, и показать, что факторкольца $F_{11}[x]/(x^2 + 1)$ и $F_{11}[x]/(x^2 + x + 4)$ изоморфны.

Тема: Теорема о примитивном элементе

Доказать, что любая конечная подгруппа мультипликативной группы F^* произвольного поля F циклична.

1. Пусть F – поле. Доказать, что если его мультипликативная группа F^* циклична, то F – конечное поле.
2. Пусть F – конечное поле и F^* - его мультипликативная группа. Доказать, что множество $H \cup \{0\}$ для любой подгруппы H группы F^* будет подполем поля F в том и только том случае, если порядок группы F^* равен 1 или простому числу вида $2^p - 1$, где p – простое число.
3. Показать, что каждый элемент конечного поля F_q характеристики p имеет в этом поле один и только один корень -й степени.
4. Показать, что если F_q – конечное поле нечетной характеристики, то элемент $a \in F_q^*$ имеет в поле F_q квадратный корень тогда и только тогда, когда $a^{(q-1)/2} = 1$.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Конечные поля» включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

№	Дата/сроки	Вид	Примерные	Форма

п/п	выполнения	самостоятельной работы	нормы времени на выполнение	контроля
I. Характеристика поля	1.09 - 28.09	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
I. Алгебраические расширения конечных полей	28.09 - 28.10	индивидуальное домашнее задание	1 неделя	Контрольная работа
I. Строение конечных полей	05.11 - 12.11	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
. Мультипликативная группа конечного поля	13.11 - 20.11	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
. Линейные рекуррентные последовательности	10.03 - 17.03	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
6) Алгебраические коды и шифры над конечными полями	20.03 - 27.04	индивидуальное домашнее задание	1 неделя	Контрольная работа Проверка ИДЗ
7) Характеристика поля	20.04 - 27.04	индивидуальное домашнее задание	1 неделя	

Рекомендации по самостоятельной работе студентов

Планирование и организация времени, отведенного на выполнение заданий самостоятельной работы.

Изучив график выполнения самостоятельных работ, следует правильно её организовать. Рекомендуется изучить структуру каждого задания, обратить внимание на график выполнения работ, отчетность по каждому заданию предоставляется в последнюю неделю согласно графику. Обратить внимание, что итоги самостоятельной работы влияют на окончательную оценку по итогам освоения учебной дисциплины.

Работа с литературой.

При выполнении ряда заданий требуется работать с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ (http://www.dvfu.ru/library/) и других ведущих вузов страны, а также доступных для использования научно-библиотечных систем.

В процессе выполнения самостоятельной работы, в том числе при написании эссе рекомендуется работать со следующими видами изданий:

а) Научные издания, предназначенные для научной работы и содержащие теоретические, экспериментальные сведения об исследованиях.

Они могут публиковаться в форме: монографий, научных статей в журналах или в научных сборниках;

б) Учебная литература подразделяется на:

- учебные издания (учебники, учебные пособия, тексты лекций), в которых содержится наиболее полное системное изложение дисциплины или какого-то ее раздела;

- справочники, словари и энциклопедии – издания, содержащие краткие сведения научного или прикладного характера, не предназначенные для сплошного чтения. Их цель – возможность быстрого получения самых общих представлений о предмете.

Существуют два метода работы над источниками:

– сплошное чтение обязательно при изучении учебника, глав монографии или статьи, то есть того, что имеет учебное значение. Как правило, здесь требуется повторное чтение, для того чтобы понять написанное. Старайтесь при сплошном чтении не пропускать комментарии, сноски, справочные материалы, так как они предназначены для пояснений и помощи. Анализируйте рисунки (карты, диаграммы, графики), старайтесь понять, какие тенденции и закономерности они отражают;

– метод выборочного чтения дополняет сплошное чтение; он применяется для поисков дополнительных, уточняющих необходимых сведений в словарях, энциклопедиях, иных справочных изданиях. Этот метод крайне важен для повторения изученного и его закрепления, особенно при подготовке к экзамену.

Для того чтобы каждый метод принес наибольший эффект, необходимо фиксировать все важные моменты, связанные с интересующей Вас темой.

Тезисы – это основные положения научного труда, статьи или другого произведения, а возможно, и устного выступления; они несут в себе больший объем информации, нежели план. Простые тезисы лаконичны по форме; сложные – помимо главной авторской мысли содержат краткое ее обоснование и доказательства, придающие тезисам более весомый и убедительный характер. Тезисы прочитанного позволяют глубже раскрыть его содержание; обучаясь излагать суть прочитанного в тезисной форме, вы сумеете выделять из множества мыслей авторов самые главные и ценные и делать обобщения.

Конспект – это способ самостоятельно изложить содержание книги или статьи в логической последовательности. Конспектируя какой-либо источник, надо стремиться к тому, чтобы немногими словами сказать о многом. В тексте конспекта желательно поместить не только выводы или положения, но и их аргументированные доказательства (факты, цифры,

цитаты).

Писать конспект можно и по мере изучения произведения, например, если прорабатывается монография или несколько журнальных статей.

Составляя тезисы или конспект, всегда делайте ссылки на страницы, с которых вы взяли конспектируемое положение или факт, – это поможет вам сократить время на поиск нужного места в книге, если возникает потребность глубже разобраться с излагаемым вопросом или что-то уточнить при написании письменных работ.

VI. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Введение	ПК-1.1 Ставит задачи, выбирает и применяет современные методы решения научных задач по тематике научных исследований, оценивает значимость получаемых результатов	Знает: новые научные результаты по выбранной тематике научных исследований	Коллоквиум (УО-2)	Вопросы к экзамену 1-5
			Умеет: правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы, оценивать значимость результатов с точки зрения их результативности и применимости	Коллоквиум (УО-2) ИДЗ	
			Владеет: навыками применения выбранных методов к решению научных задач	Индивидуальное домашнее задание (ПР-6)	
2	Характеристика поля	ПК-1.2 Критически анализирует и оценивает современные достижения и результаты деятельности по решению исследовательских и практических задач	Знает: классические и современные методы решения задач по выбранной тематике научных исследований		Вопросы к экзамену 6-10
			Умеет: осуществлять отбор, систематизацию, анализ и оценку современных достижений для решения поставленных задач	Коллоквиум (УО-2)	
			Владеет: навыками критической оценки полученных результатов для обоснования выбора оптимальной стратегии решения исследовательских и практических задач	Индивидуальное домашнее задание (ПР-6)	
3	Простые расширения конечных полей	ПК-1.3 Принимает участие и выступает на научно-тематических	Знает: способы представления научной информации при осуществлении академической и профессиональной коммуникации		Вопросы к экзамену 11-12

		конференциях	Умеет: представлять и обсуждать новые достижения и научные результаты в рамках научно-тематических конференций	Индивидуальное домашнее задание (ПР-6)	
			Владеет: навыками подготовки докладов и выступлений на научно-тематических конференциях	Коллоквиум (УО-2)	
4	Строение конечных полей	ПК-3.1 Организует деятельность учащихся, направленную на освоение программы, выбирает формы, методы и средства обучения математике, современные образовательные технологии, определяет методические закономерности их выбора	Знает концептуальные положения и требования к организации образовательного процесса по математике; особенности проектирования образовательного процесса по математике в образовательном учреждении высшего образования,	Коллоквиум (УО-2)	Вопросы к экзамену 13-14
			Умеет проектировать элементы образовательной программы, рабочую программу преподавателя по математике; формулировать дидактические цели и задачи обучения математике и реализовывать их в образовательном процессе по математике;	Коллоквиум (УО-2) ИДЗ	
			Владеет умениями по планированию и проектированию образовательного процесса	Индивидуальное домашнее задание (ПР-6)	
5	Мультипликативная группа конечного поля	ПК-3.2 Формулирует дидактические цели и задачи обучения математике и реализует их в образовательном процессе, разрабатывает программно-методическое обеспечение реализации программы обучения	Знает подходы к планированию образовательной деятельности; формы, методы и средства обучения математике	Коллоквиум (УО-2)	Вопросы к экзамену 15
			Умеет обосновывать выбор методов обучения математике и образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых	Индивидуальное домашнее задание (ПР-6)	
			Владеет методами обучения математике и современными образовательными технологиями	Индивидуальное домашнее задание (ПР-6)	
6	Линейные рекуррентные последовательности	ПК-3.3 Применяет различные средства, методы и образовательные	Знает современные образовательные технологии, методические закономерности их выбора; особенности частных	Коллоквиум (УО-2)	Вопросы к экзамену 16-18

		технологии обучения математике в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых	методик обучения математике		
			Умеет планировать и комплексно применять различные средства обучения математике	Индивидуальное домашнее задание (ПР-6)	
			Владеет методами обучения математике и современными образовательными технологиями	Индивидуальное домашнее задание (ПР-6)	
7	Алгебраические коды	ПК-1.1 Ставит задачи, выбирает и применяет современные методы решения научных задач по тематике научных исследований, оценивает значимость получаемых результатов	Знает: новые научные результаты по выбранной тематике научных исследований		Вопросы к экзамену 19
			Умеет: правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы, оценивать значимость результатов с точки зрения их результативности и применимости	Индивидуальное домашнее задание (ПР-6)	
			Владеет: навыками применения выбранных методов к решению научных задач		

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также качественные критерии оценивания, которые описывают уровень сформированности компетенций, представлены в разделе VIII.

IV. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

а) основная литература:

1. Ларин С.И. Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов по естественнонаучным направлениям / С. В. Ларин. Москва : Юрайт, 2020

https://lib.dvfu.ru/lib/item?id=chamo:884134&theme=FEFU

2. Введение в алгебраические коды : учебное пособие / Ю. Л. Сагалович. Москва : Изд-во Института проблем передачи информации РАН, 2014.
https://lib.dvfu.ru/lib/item?id=chamo:756734&theme=FEFU

3. Тропин М. П. Основы прикладной алгебры. – СПб.: Лань, 2020

https://e.lanbook.com/reader/book/139282/#1

б) дополнительная литература:

1. Чеканов С.Г., Степанова А.А. Строение конечных полей: учебно-методич. пособие / С.Г. Чеканов, Степанова А.А. - Владивосток: Издательский дом Дальневосточного федерального университета, 2013. – 28 с.
2. Р. Лидл, Г. Нидеррайтер, Конечные поля – М.: «Мир», Том 1, 2. 1988.
3. Черемушкин А.В. Теория полей. Основные свойства и уязвимости: учебное пособие. – М.: «Академия», 2009, 272 http://lib.dvfu.ru:8080/lib/item?id=chamo:291200&theme=FEFU
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:5790&theme=FEFU
5. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU
6. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-399&theme=FEFU
7. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-46&theme=FEFU
8. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:103102&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://e.lanbook.com/book/103600
Чашкин А.В., Жуков Д.А. Элементы конечной алгебры: группы, кольца, поля, линейные пространства. Московский государственный технический университет имени Н.Э. Баумана, 2016.
2. http://e.lanbook.com/books/element.php?pl1_id=56403 Игнатьев М.В. Введение в метод орбит над конечным полем: Изд-во МЦНМО.-2012

Профессиональные базы данных и информационные справочные системы

1. База данных Scopus http://www.scopus.com/home.url
2. База данных Web of Science http://apps.webofknowledge.com/

3. Общероссийский математический портал Math-Net.Ru http://www.mathnet.ru
4. Электронная библиотека диссертаций Российской государственной библиотеки http://diss.rsl.ru/
5. Электронная библиотека Европейского математического общества https://www.emis.de/
6. Электронные базы данных EBSCO http://search.ebscohost.com/

V. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Планирование и организация времени, отведенного на изучение дисциплины. Приступить к освоению дисциплины следует незамедлительно в самом начале учебного семестра. Рекомендуется изучить структуру и основные положения Рабочей программы дисциплины. Обратить внимание, что кроме аудиторной работы (лекции, лабораторные занятия) планируется самостоятельная работа, итоги которой влияют на окончательную оценку по итогам освоения учебной дисциплины. Все задания (аудиторные и самостоятельные) необходимо выполнять и предоставлять на оценку в соответствии с графиком.

В процессе изучения материалов учебного курса предлагаются следующие формы работ: чтение лекций, лабораторные занятия, задания для самостоятельной работы.

Лекционные занятия ориентированы на освещение вводных тем в каждый раздел курса и призваны ориентировать студентов в предлагаемом материале, заложить научные и методологические основы для дальнейшей самостоятельной работы студентов.

Практические занятия акцентированы на наиболее принципиальных и проблемных вопросах курса и призваны стимулировать выработку практических умений.

Особо значимой для профессиональной подготовки студентов является *самостоятельная работа* по курсу. В ходе этой работы студенты отбирают необходимый материал по изучаемому вопросу и анализируют его. Студентам необходимо ознакомиться с основными источниками, без которых невозможно полноценное понимание проблематики курса.

Освоение курса способствует развитию навыков обоснованных и самостоятельных оценок фактов и концепций. Поэтому во всех формах контроля знаний, особенно при сдаче экзамена, внимание обращается на понимание проблематики курса, на умение практически применять знания и

делать выводы.

Работа с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ и электронные библиотеки (http://www.dvfu.ru/library/), а также доступные для использования другие научно-библиотечные системы.

Подготовка к экзамену. К сдаче экзамена допускаются обучающиеся, выполнившие все задания (практические, самостоятельные), предусмотренные учебной программой дисциплины, посетившие не менее 85% аудиторных занятий.

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D732. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 45) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная.	
690922, Приморский край, г.Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корп. А (Лит. П), Этаж 10, каб.А1017. Аудитория для самостоятельной работы	Оборудование: Моноблок Lenovo C360G-i34164G500UDK – 15 шт. Интегрированный сенсорный дисплей Polymedia FlipBox - 1 шт. Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C – 1 шт.)	

Для проведения учебных занятий по дисциплине, а также для организации самостоятельной работы студентам доступно следующее лабораторное оборудование и специализированные кабинеты, соответствующие действующим санитарным и противопожарным нормам, а

также требованиям техники безопасности при проведении учебных и научно-производственных работ.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

VII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Для дисциплины «Конечные поля» используются следующие оценочные средства:

Устный опрос:

1. Коллоквиум (УО-2)

Письменные работы:

1. Индивидуальное домашнее задание (ПР-6)

Устный опрос

Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки.

Обучающая функция состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту.

Коллоквиум (УО-2) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Письменные работы

Письменный ответ приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе.

Индивидуальное домашнее задание (ПР-6) – средство для закрепления и практического освоения материала по определенному разделу.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Конечные поля»

проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – экзамен (1-й, осенний семестр). Экзамен по дисциплине включает ответы на 3 вопроса. Два вопроса носят теоретический характер, один вопрос носит практический характер.

Методические указания по сдаче экзамена

Экзамен принимается ведущим преподавателем. При большом количестве групп у одного преподавателя или при большой численности потока по распоряжению заведующего кафедрой (заместителя директора по учебной и воспитательной работе) допускается привлечение в помощь ведущему преподавателю других преподавателей. В первую очередь привлекаются преподаватели, которые проводили лабораторные занятия по дисциплине в группах.

В исключительных случаях, по согласованию с заместителем директора Школы по учебной и воспитательной работе, заведующий кафедрой имеет право принять экзамен в отсутствие ведущего преподавателя.

Форма проведения экзамена (устная, письменная и др.) утверждается на заседании кафедры по согласованию с руководителем в соответствии с рабочей программой дисциплины.

Во время проведения экзамена студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего экзамен, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Время, предоставляемое студенту на подготовку к ответу на экзамене, должно составлять не более 30 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на экзамене посторонних лиц (кроме лиц, осуществляющих проверку) без разрешения соответствующих лиц (ректора либо проректора по учебной и воспитательной работе, директора Школы, руководителя ОПОП или заведующего кафедрой), не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются на экзамен с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «отлично», или «хорошо», или «удовлетворительно», или «неудовлетворительно».

В зачетную книжку студента вносится только запись «отлично», или «хорошо», или «удовлетворительно», запись «неудовлетворительно»

вносится только в экзаменационную ведомость. При неявке студента на экзамен в ведомости делается запись «не явился».

Вопросы к экзамену

1. Строение циклических групп.
2. Кольца, гоморфизмы колец.
3. Факторкольцо и идеалы колец.
4. Теорема о факторкольце по максимальному идеалу.
5. Кольцо классов вычетов. Поле классов вычетов по простому модулю.
6. Теорема о характеристике конечного поля.
7. Кольцо многочленов над конечным полем.
8. Поле разложения многочлена.
9. Теорема о существовании и единственности конечного поля.
10. Алгоритм Евклида для многочленов.
11. Неприводимые многочлены. Основная теорема арифметики кольца многочленов.
12. Алгебраические расширения конечного поля.
13. Теорема о строении конечных полей.
14. Теорема о примитивном элементе.
15. Группа автоморфизмов конечного поля.
16. Линейные рекуррентные последовательности.
17. Матрица и характеристический многочлен линейной рекуррентной последовательности.
18. Оценка периода линейной рекуррентной последовательности.
19. Алгоритм Берлекемпа-Месси.

Критерии выставления оценки студенту на экзамене

К экзамену допускаются обучающиеся, выполнившие программу обучения по дисциплине, прошедшие все этапы текущей аттестации.

Оценка	Требования к сформированным компетенциям
«отлично»	Студент показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.

«хорошо»	Знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.
«удовлетворительно»	Фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.
«неудовлетворительно»	Незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Оценочные средства для текущей аттестации

Текущая аттестация студентов по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме контрольных мероприятий (коллоквиума, индивидуального домашнего задания) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− результаты самостоятельной работы.

Составляется календарный план контрольных мероприятий по дисциплине. Оценка посещаемости, активности обучающихся на занятиях, своевременность выполнения различных видов заданий ведётся на основе журнала, который ведёт преподаватель в течение учебного семестра.

Вопросы для коллоквиумов

1. Строение циклических групп.

2. Кольца, гоморфизмы колец.
3. Факторкольцо и идеалы колец.
4. Теорема о факторкольце по максимальному идеалу.
5. Кольцо классов вычетов. Поле классов вычетов по простому модулю.
6. Теорема о характеристике конечного поля.
7. Кольцо многочленов над конечным полем.
8. Поле разложения многочлена.
9. Теорема о существовании и единственности конечного поля.
10. Алгоритм Евклида для многочленов.
11. Неприводимые многочлены. Основная теорема арифметики кольца многочленов.
12. Алгебраические расширения конечного поля.
13. Теорема о строении конечных полей.
14. Теорема о примитивном элементе.
15. Группа автоморфизмов конечного поля.
16. Линейные рекуррентные последовательности.
17. Матрица и характеристический многочлен линейной рекуррентной последовательности.
18. Оценка периода линейной рекуррентной последовательности.
19. Алгоритм Берлекемпа-Месси.

Критерии оценивания

Оценка	Требования к сформированным компетенциям
«отлично»	Студент показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.
«хорошо»	Знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.
«удовлетворительно»	Фрагментарные, поверхностные знания важнейших

	разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.
«неудовлетворительно»	Незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Тематика индивидуальных домашних заданий

1. Построение факторкольца по кольцу полиномов над конечным полем
2. Поиск неприводимых и примитивных полиномов над конечным полем.
3. Построение конечного расширения поля.
4. Оценка периода линейной рекуррентной последовательности

Критерии оценки индивидуальных домашних заданий

Оценка	Требования
«зачтено»	Студент выполняет индивидуальное домашнее задание в полном объёме с соблюдением необходимой последовательности проведения измерений, правильно самостоятельно определяет цель работы; самостоятельно, рационально выбирает необходимое оборудование для получения наиболее точных результатов проводимой работы. Грамотно и логично описывает ход работы, правильно формулирует выводы, точно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления и т.п., умеет обобщать фактический материал. Допускается два/три недочёта или одна негрубая ошибка и один недочёт. Работа соответствует требованиям и выполнена в срок.
«не зачтено»	Студент выполнил индивидуальное домашнее задание не полностью, объём выполненной части не позволяет сделать правильные выводы; не определяет самостоятельно цель работы; в ходе работы допускает одну и более грубые ошибки, которые не может исправить, или неверно производит наблюдения, измерения, вычисления и т.п.; не умеет обобщать фактический материал. Индивидуальное домашнее задание не выполнено.